

ABSTRACT OF THE DISCLOSURE

A system provides an order-invariant fuzzy commitment scheme. In an exemplary embodiment, the scheme includes receiving a first set of elements and selecting a polynomial for encoding an item under the first set of elements to generate an order-invariant fuzzy commitment of the item. The system utilizes an error-correcting code for decommitting the item if a second set of elements has a specified level of overlap with the first set of elements.

10 RSA-502AUS PATENT APPLICATION